

**Response Update**  
**Corrective Action Plan (CAP): Audit Report #06DP-05**  
**Data Center Review**  
**Department of Administration**  
**August 20, 2010**

| Agency       | Recommendation #  | Does this affect a federal program? | CFDA # (if previous YES) | Management View | CAP – Corrective Action Plan  | Person responsible for CAP | Target Date                   |
|--------------|---|-------------------------------------|--------------------------|-----------------|---|----------------------------|-------------------------------|
| 61010<br>DOA | <b>Recommendation #1</b><br>We recommend the Department of Administration (DOA) and the Information Technology Services Division:   | No                                  |                          | Concur          | A. The currently-fragmented inventories of equipment, systems and data will be consolidated, updated and maintained.<br><b>Near-term:</b> Centralized Technical Services will address the issues.   | Dave Harris                | <b>Completed</b><br>9/30/2006 |
|              | A. Maintain and update the inventory of equipment, systems, and data residing in the data center.   |                                     |                          |                 | <b>Long-term:</b> the Configuration DB within ITSD's Service Mgmt System will be the single reference point for this information. This effort will take place after the initial move to the Helena Data Center.   | Wendy Wheeler              | 12/31/2010                    |
|              | B. Coordinate with all agencies that have hosted systems in the data center to rank the system's criticality and establish a priority for the order in which systems will be brought back up. |                                     |                          |                 | B. The Department will work with agencies on "Continuity of Government (COG)/Continuity of Operations (COOP)" plans, and will pay particular attention to their recovery plan for critical systems residing in the data center. This ongoing process has been defined and agencies are participating. | Dawn Pizzini               | <b>Completed</b>              |

| Agency | Recommendation #  | Does this affect a federal program? | CFDA # (if previous YES) | Management View | CAP – Corrective Action Plan  | Person responsible for CAP   | Target Date  |
|--------|---|-------------------------------------|--------------------------|-----------------|---|--|--|
|        | C. Evaluate existing threats to the data center including the potential impact or harm.<br><br>D. Conduct a cost analysis associated with implementing or improving controls. |                                     |                          |                 | <p>The "48 hour" plan was replaced by the development of the COOP/COG plans. The COG plan is in place and the Continuity Management Plan is under development. Ongoing COOP planning is in process with the agencies.</p> <p>C. The Department will conduct a threat and impact assessment for the data center by participating in the Capitol complex vulnerability assessment scheduled for July</p> <p>D. The state legislature approved funding to build a replacement data center for the State of Montana. This facility is being constructed as a Tier III data center with a significant focus on security. The location of the new data center was selected for a number of security reasons. All specific risks identified regarding the data center in the Mitchell building will no longer be relevant.</p> <p>Construction of the new Helena Data Center is complete. Systems are being moved and all will be housed in the new data center by</p> | <p>Dawn Pizzini</p> <p>Pat Boles</p> <p>Lynne Pizzini</p> <p>Lynne Pizzini</p> | <p><b>Completed</b></p> <p><b>Completed</b><br/>8/31/2006</p> <p><b>Completed</b><br/>01/01/2010</p> <p>12/13/2010</p> |



| Agency | Recommendation #   | Does this affect a federal program? | CFDA # (if previous YES) | Management View | CAP – Corrective Action Plan   | Person responsible for CAP   | Target Date   |
|--------|--|-------------------------------------|--------------------------|-----------------|--|--|---|
|        | background checks are completed.<br><br>C. Follow policy and maintain required authorization documentation of file for each individual who has card access to the data center.<br><br>D. Conduct a periodic review of all key card access to the data center to confirm appropriateness.<br><br>E. Monitor and review the card key activity logs and data center visitor logs for inappropriate or unauthorized access.<br><br>F. Develop a system to ensure operator awareness of physical security breaches. |                                     |                          |                 | <p>assure required background checks are performed for individuals and positions that handle sensitive information housed in the data center.</p> <p>C. The Department will maintain card key authorization documentation as recommended.</p> <p>D. The Department will formalize the access card review frequency and process.</p> <p>E. The Department will review the logs as recommended. The Department will also establish and communicate guidelines for visitor access to the data center.</p> <p>F. The Department will develop a system to ensure data center operators are alerted of physical security breaches.</p> <p>A new software system is being implemented for the Mitchell Building as well as the new data center. This software will allow operators to monitor physical security and send notification</p> | <p>Mike Krings</p> <p>Mike Krings</p> <p>Mike Krings</p> <p>Mike Boyer</p> | <p><b>Completed</b></p> <p><b>Completed</b><br/>8/31/2006</p> <p><b>Completed</b><br/>7/15/2006</p> <p><b>Completed</b><br/>2/28/2010</p> <p>09/01/2010</p> |

| Agency    | Recommendation #  | Does this affect a federal program? | CFDA # (if previous YES) | Management View | CAP – Corrective Action Plan   | Person responsible for CAP          | Target Date  |
|-----------|---|-------------------------------------|--------------------------|-----------------|--|-------------------------------------|--|
|           |   |                                     |                          |                 | breaches. The SMDC has intrusion detection and video surveillance throughout. Door alarm alerts are directed to the EOC, which has video access. These components are being installed during the month of August 2010.   |                                     |  |
| 61010 DOA | <b>Recommendation #3</b><br>We recommend the Department strengthen safeguards to mitigate the risks associated with earthquake and water-related threats. |                                     |                          | Concur          | <p>During the budget planning process for FY06-07, the Department submitted an EPP for earthquake dampening devices for data center equipment to provide protection during “non-catastrophic” earthquakes. That proposal did not survive the previous budget process. The Department will resubmit that EPP to provide a measure of earthquake protection ISO-Base cabinet seismic protection has been installed on all Helena SMDC cabinets to assure survival of the equipment within the “500-year seismic event” building.</p> <p>The Department has installed new water-sensing and alert equipment in the data center.</p> | <p>Mike Boyer</p> <p>Mike Boyer</p> | <p><b>Completed</b></p> <p>Earthquake protection equipment was not included in HB2 when passed; however, the new buildings are engineered as “critical structures”</p> <p><b>Completed</b></p> |
| 61010 DOA | <b>Recommendation #4</b><br>We recommend the Department:<br>A. Maintain an updated statewide  |                                     |                          | Concur          | A. GSD has oversight responsibility for the COG plan   | Sheryl Olson                        | <b>Completed</b><br>7/1/06   |

| Agency    | Recommendation #  | Does this affect a federal program? | CFDA # (if previous YES) | Management View | CAP – Corrective Action Plan   | Person responsible for CAP | Target Date                  |
|-----------|---|-------------------------------------|--------------------------|-----------------|--|----------------------------|------------------------------|
|           | disaster recovery plan.   |                                     |                          |                 | ITSD is responsible for developing and maintaining the disaster recovery plan for ITSD equipment and services. Process has been established to accomplish the continual review and updating of disaster recover plans.       | Lynn Pizzini               | <b>Completed</b>             |
|           |   |                                     |                          |                 | ITSD is also responsible to provide technical support for the software tool used to develop and maintain COOP plans on a statewide basis. This ongoing process has been established and is underway with the state agencies. | Dawn Pizzini               | <b>Completed</b>             |
|           | B. Coordinate with the Governor's office to request that agencies assign a higher priority to disaster recovery.                |                                     |                          |                 | B. The Governor's office has placed a high priority on disaster recovery and set expectations for agency participation in COG/COOP planning efforts  | Dick Clark                 | <b>Completed</b>             |
| 61010 DOA | We recommend the Department clearly define and designate responsibility for coordination of all aspects of data center security |                                     |                          | Concur          | ITSD and GSD established a protocol to control authorization of access to the data center that improves strength in the security center.   | Dick Clark                 | <b>Completed</b><br>1/2/2007 |